Random Graph Models for Wireless and Social Networks

[Keynote Talk Abstract]

Matthias Grossglauser
School of Computer and Communication Sciences
EPFL
Lausanne, Switzerland
matthias.grossglauser@epfl.ch

ABSTRACT

Operating large-scale social applications over opportunistic wireless networks entails many fascinating engineering challenges. We strive for robust and efficient algorithms for specific problems like opportunistic forwarding, routing, or publish-subscribe, and we want to ascertain global properties like security, privacy, fairness, and high performance. One particular set of challenges concerns the scalability of this whole endeavor: is it fundamentally possible for such applications and underlying methods to scale up to large networks, without jeopardizing desirable system properties?

We discuss recent progress in some of the key problems in this area at three conceptual layers: opportunistic forwarding, routing under mobility, and social network privacy.

Opportunistic forwarding exploits the random broadcast nature of the wireless channel and the availability of multiple "good" routes towards a destination. This approach can deliver a message to its destination at a potentially lower expected cost than over a single shortest path. We introduce a forwarding algorithm and associated "anypath metric" that is optimal, building on the observation that no single-path metric can achieve optimality in general.

In routing under mobility, the key challenge is to keep track of the changing network topology, so that efficient routes can be computed at any time between any pair of nodes. We ask whether there exist low-overhead schemes that produce low-stretch routes, even in large networks where all the nodes are mobile. We present a scheme that maintains a hierarchical structure within which constant-stretch routes can be efficiently computed between every pair of nodes. The scheme rebuilds each level of the hierarchy periodically, at a rate that decreases exponentially with the level of the hierarchy, and achieves constant stretch under a mild smoothness condition on the mobility process.

Finally, we address the problem of the privacy of an anonymized social network. The specific challenge is the sharing or public release of anonymized network data without accidentally leaking personally identifiable information (PII). Unfortunately, it is often difficult to ascertain that sophisticated statistical techniques, potentially employing additional external data sources, are unable to break anonymity. We show an asymptotic condition, based on a random graph model, under which a computationally powerful adversary would be able to re-identify the anonymized node identities. This has important implications for privacy policies in social network structures.

What binds the above problem formulations and results together is our reliance on stochastic network models that retain only the salient features of each problem. These abstractions allow us to make precise statements about scalability to very large systems. We hope that these results complement and inform more focused work on methods, protocols, and applications for mobile, opportunistic, and social networks.

MobiOpp 12, March 15–16, 2012, Zürich, Switzerland.